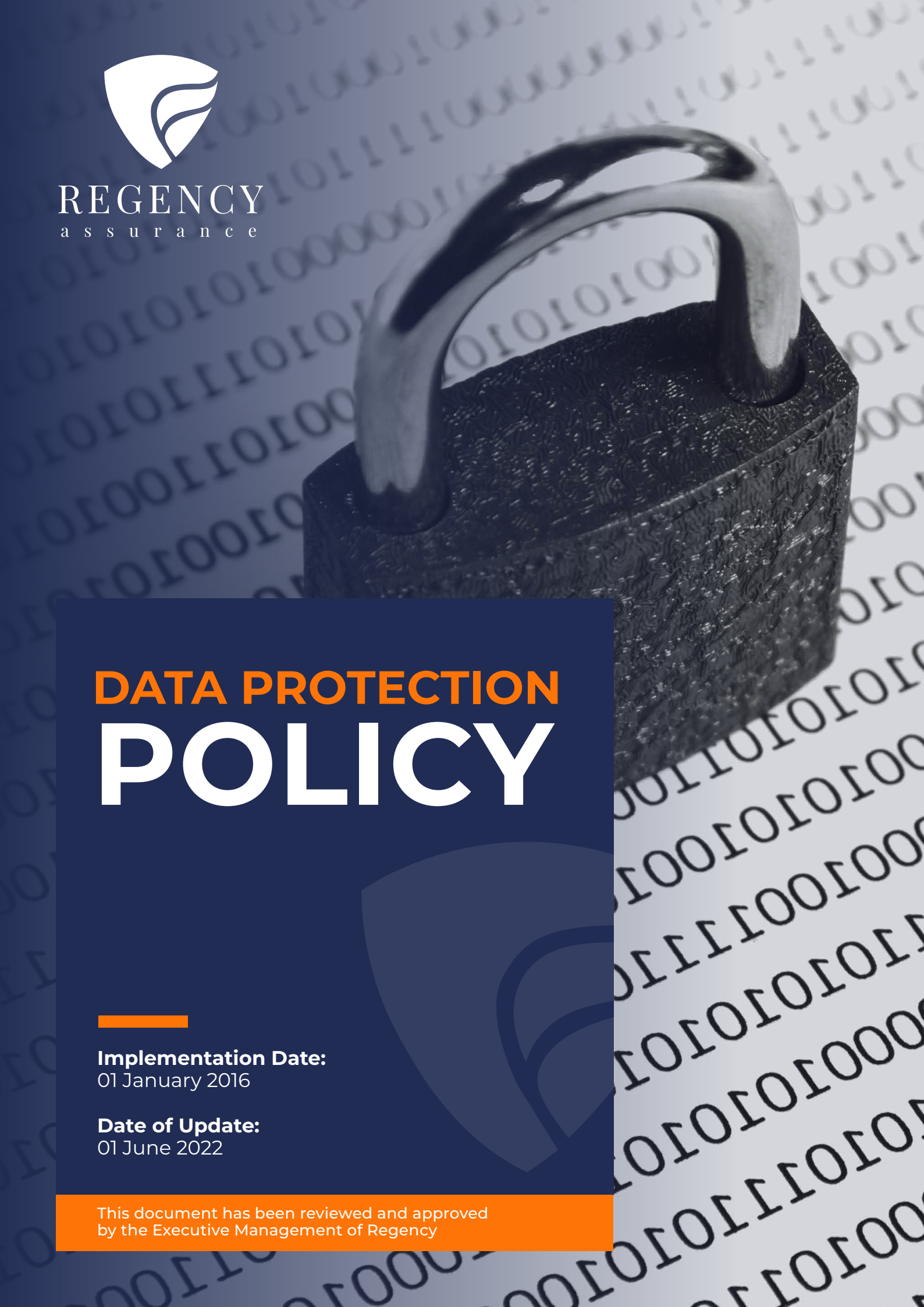
REGENCY
assurance



DATA PROTECTION POLICY

Implementation Date:
01 January 2016

Date of Update:
01 June 2022

This document has been reviewed and approved by the Executive Management of Regency

REGENCY
assurance

DATA PROTECTION POLICY

Table of Contents:

INTRODUCTION

Regency believes that good business ethics are integral to defining who the firm are and what the firm does. Regency endeavours to be professional and accountable in everything that the firm does and further strive to discharge its responsibilities in an ethical and lawful manner.

This policy governs how Regency handles the Personal Data of our customers, affiliates, employees, and other third parties.

Given the nature of the business operations conducted by Regency, we shall be required as part of routine business activities to collect and process Personal Data. This may include data we receive directly from a client (for example, by completing forms or through corresponding with us by phone, email, or other means) and data we receive from other sources (including, for example, third party insurance brokerages, medical facilities etc.).

Regency recognises that the correct and lawful treatment of data will maintain confidence in our company and will provide for successful business operations. Regency also recognises that Personal Data loss or misuse may potentially result in harm to individuals, including embarrassment, inconvenience, and fraudulent data use. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that Regency regards as imperative to the successful functioning of the company.

Any third-party affiliates or sub-contractors which from time to time may be engaged by Regency shall be required to read and comply with this policy when processing Personal Data on our behalf. Any breach of this policy or related guidelines, operating procedures, or processes designed to protect Personal Data, whether by Regency, their employees, affiliates or third parties may result in disciplinary action, indemnity or any other remedy as Regency may determine appropriate in the circumstances, including termination of any contractual agreement.

All Regency personnel with Personal Data access or responsibility for supervising personnel with Personal Data access must read this policy and at all times act in accordance with its requirements. Any failure to do so may result in disciplinary action, and depending on the circumstances, termination of employment.

POLICY SCOPE

This policy applies to all Personal Data we collect, maintain, transmit, store, retain, or otherwise use, regardless of the media on which that data is stored or whether it relates to employees, clients, or any other Data Subject. Personal Data is subject to certain legal and other useful international guidance and best practice standards.

This policy, and any other documents referred to in it, sets out the basis on which our employees, agents, and representatives, including third-party service providers and affiliates who have access to the Personal Data we hold, will process any Personal Data we collect from Data Subjects, or that is provided to us by Data Subjects or other sources. Regency has policies, procedures and training in place in respect of data protection, confidentiality and information security. Such measures are regularly reviewed with the objective of ensuring their continuing effectiveness.

This policy sets out the Personal Data protection rules and conditions that Regency shall follow when obtaining, handling, processing, transferring, or storing Personal Data.

The Data Protection Officer (DPO) is responsible for ensuring compliance with all Applicable Legislation and with the terms of this policy. The DPO is also responsible for administering and overseeing implementation of this policy and, as applicable, developing related operating procedures, processes, policies, notices, and guidelines.

Regency also maintains a current and comprehensive Privacy Policy relating to the use of Regency websites, as hosted by Regency Assurance. This privacy notice details how Regency collects and processes Personal Data through the use of the website, including any such data that may be voluntarily disclosed by service users when making an enquiry, request, or submitting any type of information to Regency. This Privacy Policy can be accessed and read in its entirety here: https://www.regencyassurance.com/privacy-policy

RELEVANT LAWS

This policy has been developed in accordance with the following Data Protection Laws and Regulations of St. Kitts and Nevis:

- Data Protection Act, 2018;
- The Constitution of St Kitts and Nevis, 1983.

In addition to the above-mentioned legislation, the international standards and recommendations developed by the following agencies were used to guide the material provided in the policy, which are used as a guideline rather than being expressly adopted verbatim. The additional standards include but are not limited to specifically but not limited to:

- ISO 27001;
- General Data Protection Regulation (GDPR).

DEFINITIONS OF DATA PROTECTION TERMS

"Data Subject" means the individual about whom we hold Personal Data. Given the nature of the business as a long-term licenced insurance company operating worldwide, Data Subjects may be nationals or residents of any country.

"Personal Data" means information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) said subject from that data alone or in combination with other data we possess or can reasonably access. Personal Data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or conduct.

"Sensitive Personal Data" includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition, sexual life, criminal proceedings or genetic data. Sensitive Personal Data also includes financial account or credit information, credit or debit card number, security access code or other cardholder details. Processing Sensitive Personal Data can only occur under strict conditions.

"Processing" means any activity that involves the use of Personal Data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Data to third parties.

"Security incident" means any act or omission that compromises the security, confidentiality, integrity, or availability of Personal Data or the physical, technical, administrative, or organisational safeguards that we or any third-party service providers put in place to protect it. The loss of or unauthorised access, disclosure, or acquisition of Personal Data is a security incident.

"Data Controller" is the person or organisation that determines when, why, and how to process Personal Data. It is responsible for establishing practices and policies in line with the Applicable Legislation. Regency is the Data Controller of all Personal Data used in our business for our own commercial purposes. When referring to Regency as the Data Controller, or with any reference to "we", "us" or "our", such references relate to Regency Assurance, and any and all subsidiary entities thereof, including but not limited to Regency for Expats, Regency Employee Benefits and Regency Financial Services.

PERSONAL DATA PROTECTION PRINCIPLES

Regency adheres to general data privacy principles when collecting and processing Personal Data that require us to:

(a) Collect and use Personal Data fairly and only for lawful and specified purposes related to our legitimate business objectives;

(b) Limit our Personal Data collection to what is adequate, relevant, and not excessive for the intended purpose;

(c) Make information about our Personal Data processing practices available and easily-accessible and present the same in a clear and transparent manner;

(d) Ensure or take all reasonable steps to ensure the accuracy of the Personal Data we collect, hold, and use;

(e) Retain Personal Data only for the time needed to fulfil the established purpose;

(f) Respect Data Subjects' rights;

(g) Secure the Personal Data we hold.

SPECIFIED BUSINESS PURPOSES

Any employees, agents, affiliated individuals or third-party engaged by the business may only access Personal Data when a specific business need requires such data to be accessed. Employees, agents, affiliated individuals or third-parties engaged by the business cannot access Personal Data for any reason unrelated a specific business need.

Regency may only collect and process Personal Data for specified purposes which are reasonably necessary to accomplish our legitimate business objectives. Applicable legislation may further restrict our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Personal Data processing, but to ensure that we process Personal Data fairly and without adversely affecting the Data Subject's rights. Lawful processing grounds may include but are not limited to the following:

(a) Where the Data Subject has unambiguously consented, or given express authorisation when required;

(b) Where it is necessary to facilitate our agents, partners, subsidiaries or affiliates to perform services for us as required by the legitimate interests of the business;

(c) The processing is necessary for the creation, engagement, issuance or performance of a contract with the Data Subject;

(d) Where processing is required to meet our legal compliance obligations;

(e) It is disclosed to entities that perform marketing services on our behalf or those with whom we have joint marketing agreements

(f) Where necessary to protect the Data Subject's vital interests;

(g) Where the processing is necessary on the part of Regency, or any affiliated entities or third-parties, to facilitate the effective functioning, review or evaluation of any Regency product;

(h) In the event of any invitation to treat, or in the event of any discussion, offer or negotiation to enter into a contract or any form of commercial relationship with Regency where Personal Data is required to determine the specific conditions, warranties, details or functioning of such an agreement.

Regency shall not use Personal Data for new, different, or incompatible purposes to those outlined above or in the general fulfilment of the legitimate aims of the business unless the Data Subject consents explicitly to the new usage.

When processing Sensitive Personal Data, Regency must meet any additional conditions as required by the Applicable Legislation, such as explicit Data Subject consent.

NOTIFYING DATA SUBJECTS

Whenever Regency collects Personal Data directly from Data Subjects, including for contractual or claims management purposes, this policy informs how and why we will use, process, disclose, protect, and retain that data. This policy will also identify Regency as the Data Controller and provide our contact information as follows: info@regencyassurance.com

When Regency collects Personal Data directly from Data Subjects, we will provide such subjects with information about how and why we will use, process, disclose, protect, and retain their Personal Data through this policy. If Regency receives Personal Data about a Data Subject from other sources, such as third-parties or affiliated entities, Regency will provide the Data Subject with this information as soon as possible thereafter.

Please contact the DPO if you are unsure whether a specific use is appropriate, you have any questions regarding this policy and how it applies to collected Personal Data.

SHARING PERSONAL DATA

Regency may only share the Personal Data we hold with another employee, agent, or representative of our group, which includes subsidiaries and affiliates, if the recipient has a specific need to know the information and the transfer complies with any applicable cross-border transfer restrictions (see Cross Border Personal Data Transfers).

Regency shall only be entitled and authorised to share the Personal Data of any Data Subject with third parties if all the following conditions apply:

(a) They have a need to know the information for the purposes of providing the contracted services;

(b) Sharing the Personal Data complies with this policy which is provided to the Data Subject and, if required, the Data Subject's specific consent has been obtained;

(c) Regency is satisfied that the recipient has adequate and suitably sophisticated data protection policies, procedures and mechanisms in place to ensure the protection of the Data Subject´s data and ensure it is used only for authorised purposes;

(d) The transfer complies with any applicable cross border transfer restrictions (see Cross Border Personal Data Transfers).

Regency may also share a Data Subject's Personal Data with third parties if in receipt of the prior approval of the DPO indicating that special circumstances apply, such as for a disclosure required to comply with legal obligations, enforce or apply a contract or other agreement with the Data Subject, to protect the safety of our employees, customers or others, or to protect our rights or property. This includes exchanging information with third parties for the purposes of fraud protection, anti-bribery or anti-money laundering purposes and credit risk reduction.

If any employees, affiliates, agents or third-parties instructed by Regency are unsure about whether a specific disclosure is appropriate or allowed, they must consult with the DPO and obtain authorisation for such a disclosure.

CROSS-BORDER PERSONAL DATA TRANSFERS

Cross-Border Personal Data transfers occur where the Personal Data of a Data Subject which originates in one country is transmitted across borders to another person, entity or organisation for such party to view, access or handle the data in a different country.

Regency may only transfer Personal Data on a cross-border basis if one of the following requirements is met:

(a) The transfer is required for the effective creation, arrangement or functioning of any contract, product or agreement in place between Regency and the Data Subject;

(b) The transfer is required to facilitate Regency, or any affiliate, agent, partner or third-party to effectively execute their rights under any agreement or contract in place with the Data Subject;

(c) Where it is necessary to allow our agents or partners to provide services for us;

(d) Where the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(d) The Data Subject provides informed consent for the transfer;

(e) The DPO concludes that the transfer complies with all relevant cross-border transfer restrictions and approves it in writing.

DATA ACCURACY

Regency shall place reliance upon the Data Subject to ensure that any Personal Data which is disclosed to Regency by the Data Subject which Regency use and hold is accurate, complete, up to date, and truthful to the best knowledge and belief of the Data Subject. Where incorrect, misleading or factually incorrect data is supplied by a Data Subject to Regency, this may affect, invalidate or lead to breach of any agreement in place between Regency and the Data Subject.

In the event that any Personal Data is disclosed to Regency by an affiliate or third party on behalf of a Data Subject, Regency shall exercise all reasonable effort to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Regency will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

DATA RETENTION

Regency will not keep Personal Data longer than needed for legitimate business purposes or purposes for which we originally collected it, and shall take all reasonable steps to destroy, or erase from our systems, all Personal Data that we no longer require, and follow all applicable records retention practices and procedures.

DATA SECURITY

Regency is responsible for protecting any Personal Data which we hold and will take reasonable and appropriate security measures against the unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Regency will exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use, or disclosure.

Regency shall follow all practices and procedures which are put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Regency may only transfer Personal Data to third-party service providers where Regency is satisfied of their ability to protect the Personal Data of subject with sufficiently secure and sophisticated policies and procedures in place as determined by Regency.

Regency shall maintain data security by protecting the confidentiality, integrity, and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the data can access it;

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed;

(c) Availability means that authorised users are able to access the data when they need it for authorised purposes.

Regency will develop, implement, and maintain safeguards appropriate to:

(a) Our size, scope, business, and available resources;

(b) The amount and nature of Personal Data that we control or maintain;

(c) The identified risks associated with the Personal Data.

REPORTING SECURITY INCIDENTS

If Regency or an employee thereof, affiliate, third-party or Data Subject suspect that a security incident has occurred, the DPO shall be informed. Regency have put in place procedures to deal with any suspected Personal Data breach and will notify the Data Subject and any applicable regulator of a breach where we are legally required to do so.

DATA SUBJECTS´ RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These rights vary depending on the specific circumstances of their relationship with Regency, but may include rights to:

(a) Request access to their Personal Data that we hold;

(b) Prevent our use of their Personal Data for direct marketing purposes;

(c) Ask us to delete Personal Data or correct inaccurate data (see also Data Accuracy);

(d) Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else, unless a legitimate business need or legal justification exists to do.

Data Subjects must make a written request to access, correct, or delete the Personal Data we hold about them. Upon receipt, Regency shall forward any written Data Subject request to the DPO who will review, evaluate and respond to the request within 21 days of receipt. Regency shall be entitled to charge a small fee relating to the time and administrative costs of reviewing, collating and responding to any such written request.

CHANGES TO THIS POLICY

Regency reserves the right to change this policy at any time. We last revised this policy on 01 June 2022.

www.regencyassurance.com
info@regencyassurance.com